Saturn Studio – Gestión de Credenciales



El sistema de gestión de credenciales de **Saturn Studio** permite almacenar de forma segura las claves de acceso a diversos servicios, como **OpenAI, Gmail y bases de datos**, entre otros. Con las funcionalidades actuales, es posible colaborar en equipo sin comprometer la seguridad de los datos sensibles y flexibilizar el uso de los bots mediante variables dinámicas.

Credenciales Compartidas (Shared Credentials)

Las credenciales compartidas permiten otorgar acceso a otros usuarios o equipos sin necesidad de enviar contraseñas o llaves maestras de forma directa.

Beneficios Clave

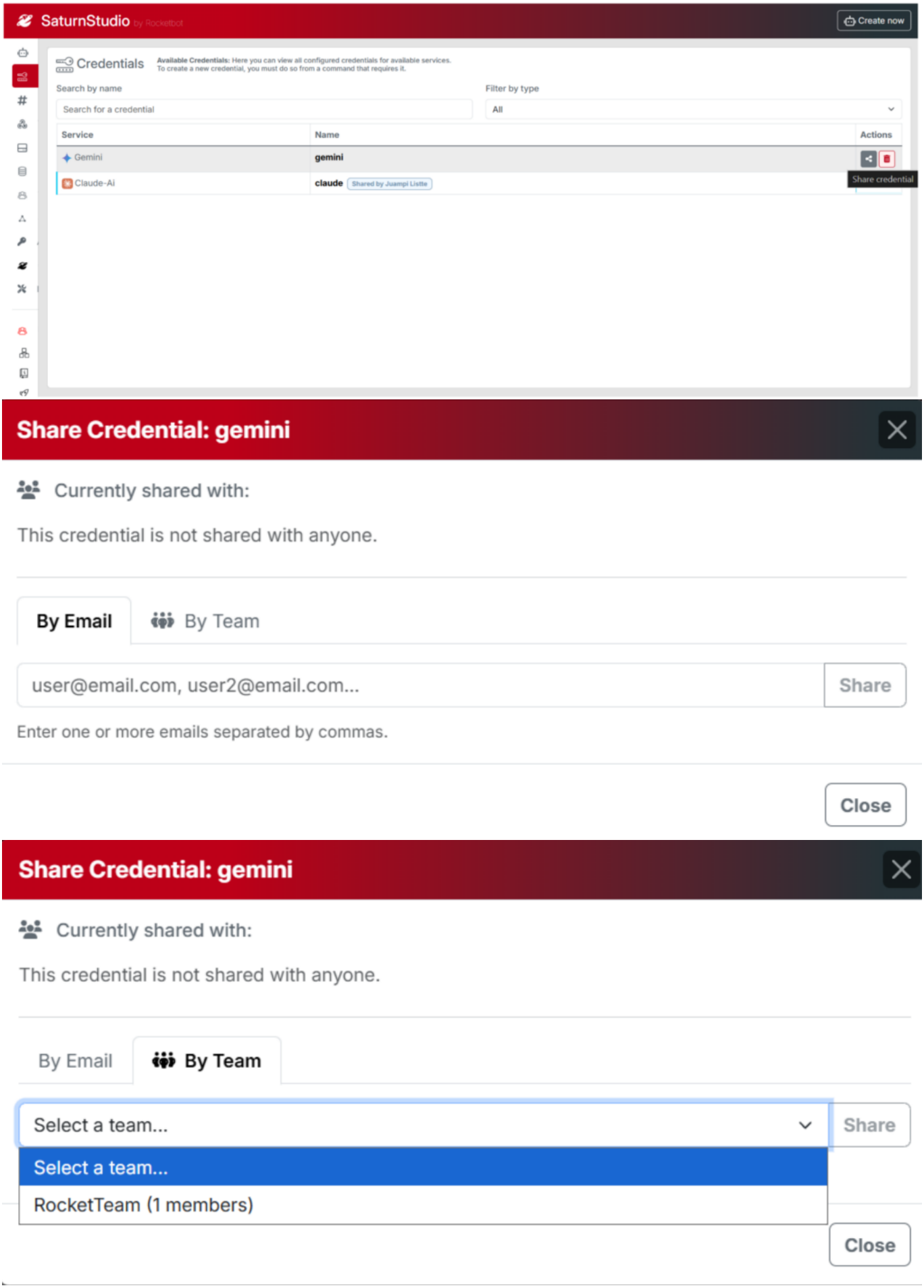
Beneficio	Descripción
Seguridad	Los datos sensibles (API keys, contraseñas) nunca se exponen al receptor.
Control Total	El propietario puede revocar el acceso en cualquier momento.
Eficiencia	Ideal para equipos que requieren utilizar los mismos servicios de forma unificada.

Cómo compartir una credencial

1. Navegue a la sección **Credentials** en Saturn Studio.
2. Identifique la credencial en la lista y haga clic en el icono de **Compartir**.
3. Seleccione el método de envío:
    - **Por Email:** Ingrese uno o más correos separados por comas y haga clic en **Share**.
    - **Por Equipo:** Elija el equipo del menú desplegable y haga clic en **Share** (todos los miembros recibirán acceso automáticamente).

Los usuarios recibirán una notificación por email informándoles que

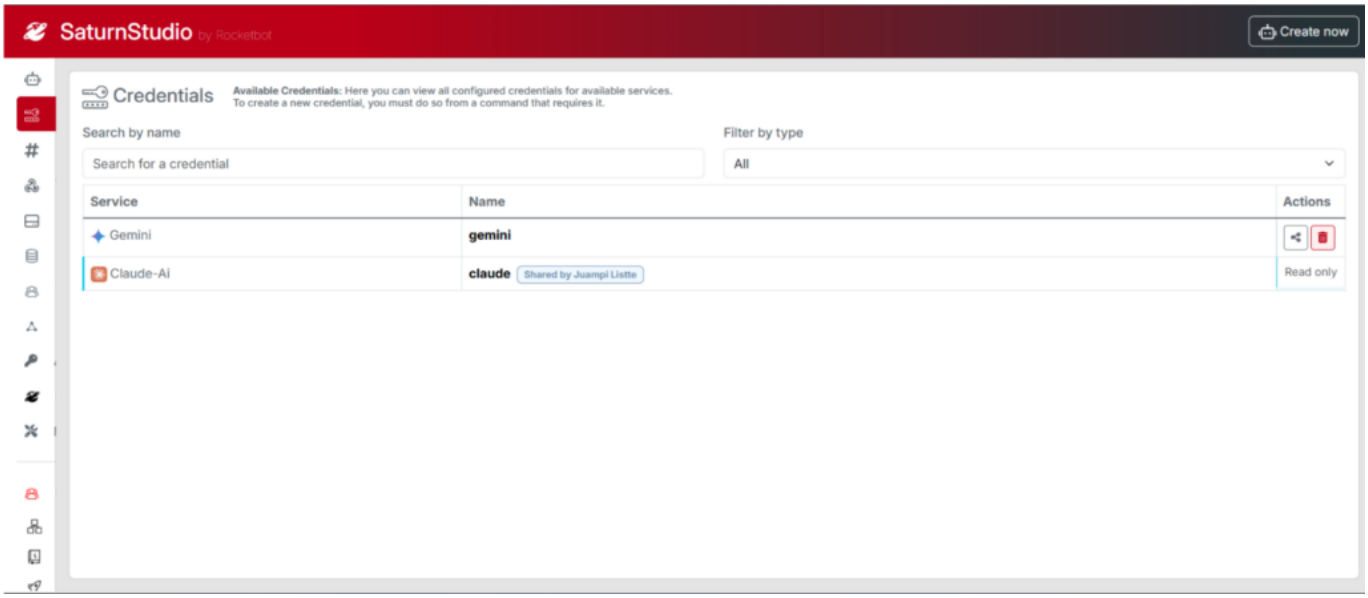
tienen una nueva credencial compartida.



Visualización de Credenciales Recibidas

Cuando un usuario o equipo comparte una credencial con usted, esta se integra automáticamente en su entorno de trabajo con las siguientes características visuales y operativas:

Elemento	Descripción Técnica
Identificación	Aparecen en su listado general de **Credentials** con un distintivo azul que indica "Shared by [Nombre]".
Uso en Bots	Puede utilizarlas en cualquier comando de sus robots de la misma forma que una credencial propia.
Restricción de Seguridad	Son de **Solo Lectura (Read Only)**. El receptor tiene prohibido editar los valores internos o eliminar la credencial del sistema.



Revocación de Acceso (Propietario)

Si usted es el dueño de la credencial, tiene la potestad de retirar el acceso a cualquier colaborador o equipo de forma inmediata siguiendo estos pasos:

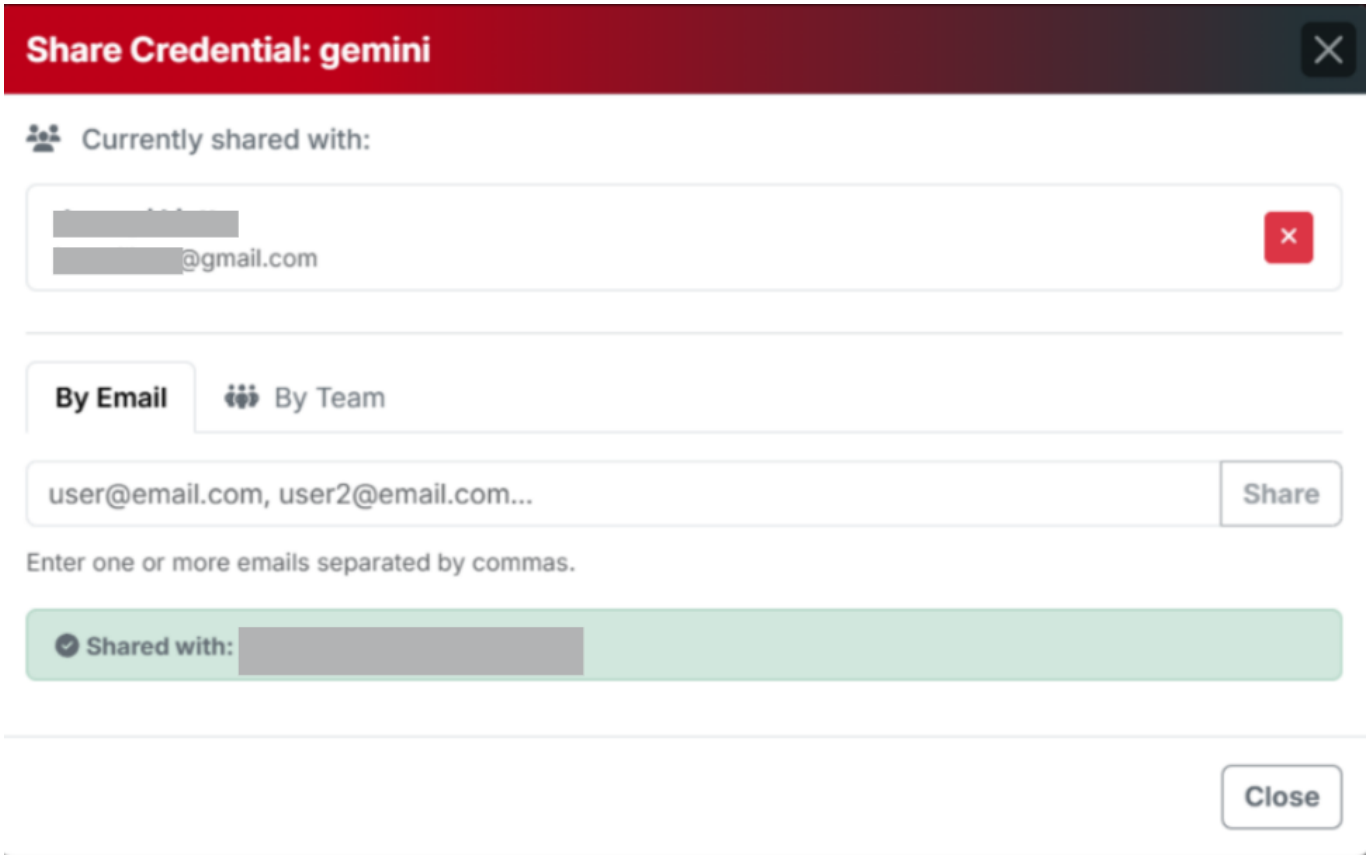
1. Diríjase a la sección **Credentials** y localice la credencial que desea gestionar.
2. Haga clic en el icono de **Compartir** para abrir el modal de gestión.
3. Ubique la lista de usuarios en el apartado **“Currently shared with”**.

Gestión de permisos

Acción	Procedimiento	Resultado
Quitar Acceso	Haga clic en la **X** roja situada al lado del correo del usuario o nombre del equipo.	El acceso se revoca al instante y el receptor ya no podrá visualizar ni usar la credencial en sus procesos.

Acción	Procedimiento	Resultado
Confirmación	El sistema mostrará un mensaje de éxito indicando que el acceso ha sido removido.	El usuario desaparece de la lista de colaboradores autorizados.

> **Efecto Inmediato:** Al revocar el acceso, cualquier robot del receptor que dependa de esa credencial fallará en su próxima ejecución, ya que la llave de acceso dejará de ser válida para ese usuario.



Variables tipo Credencial

Estas variables almacenan una referencia a una credencial en lugar de un valor estático, lo que permite parametrizar el comportamiento del bot sin modificar sus comandos internos.

Escenarios de Uso

- Cambiar rápidamente la credencial que utiliza un bot.
- Alternar entre diferentes entornos, como **Desarrollo y Producción**.
- Parametrizar servicios sin editar el flujo de trabajo.

Configuración

1. En el editor del robot, vaya a **Variables** y seleccione **Add Variable**.
2. Defina el **Name** (ej. mi_conexion_db) y en **Type** seleccione **Credential**.
3. Complete los campos técnicos:
    - **Select Module:** El servicio correspondiente (OpenAI, Gmail, etc.).
    - **Credential:** Seleccione la credencial específica a referenciar.

4. Para utilizarla en un comando, escriba el nombre de la variable entre llaves en el campo de credencial: {mi_conexion_db}.

Casos de Uso Prácticos

Colaboración en Equipo: Un líder de equipo crea una API Key de OpenAI, la comparte “By Team” y todos los miembros pueden usarla en sus bots. Si la clave cambia, solo el líder necesita actualizarla en un único lugar.

Ambientes Múltiples: Puede crear una variable llamada db_connection. En desarrollo apunta a la base de pruebas y en producción simplemente se reasigna a la base real sin tocar el código del bot.

Centralización de Servicios: Ideal para cuando varios bots usan el mismo servicio (ej. Email). Crea una única credencial global y vincúlala mediante variables en cada robot; si la clave cambia, solo la actualizas en un lugar y todos los procesos se sincronizan automáticamente.

Preguntas Frecuentes

Pregunta	Respuesta
¿Puedo ver los datos sensibles de una credencial compartida?	No. Solo puede usarla; las contraseñas permanecen ocultas.
¿Qué pasa si el propietario elimina la credencial?	El acceso se pierde automáticamente y los bots que la usen fallarán hasta configurar una nueva.
¿Puedo compartir una credencial que compartieron conmigo?	No. Solo el propietario original tiene permisos de compartición.
¿Las variables funcionan con credenciales compartidas?	Sí, puede crear una variable que apunte a una credencial que alguien más compartió con usted.